October 28-29, 2013 -- NSA has only itself to blame for leaks

publication date: Oct 27, 2013
Previous | Next

October 28-29, 2013 -- NSA has only itself to blame for leaks

At the outset of the English-speaking signals alliance after World War II, there were only five countries involved in carrying out signals intelligence operations: the United States, the United Kingdom, Canada, Australia, and New Zealand. This alliance was based on the UK-USA Agreement of 1946 that had its actual roots during World War II and the BRUSA (Britain-U.S.) agreement of 1943.

During the Cold War era, the four non-U.S. English-speaking SIGINT alliance countries, known as "Second Parties," as opposed to the U.S. (the First Party), managed to keep their operations largely secret. Soon, agreements to share signals intercepts with NSA, were concluded with "Third Parties." Third parties were non-English speaking countries that were allies of the United States. The sharing was largely one-way, with Third Parties providing more to NSA than what they received in return. NSA "product" was usually highly-sanitized analysis reports. Third Parties originally included countries like Denmark, Norway, the Netherlands, and West Germany. Later, such countries as Japan, South Korea, Turkey, Greece, Italy, Spain, and Portugal joined the Third Party partners.

France, which withdrew from NATO's military structure in 1967 and which carried out intelligence operations against the United States, was kept distant from the NSA partnership. However, France gradually became a Third Party, especially after French President Nicolas Sarkozy returned France to NATO's military fold in 2009.

Israel, which was considered a hostile intelligence nation by U.S. counterintelligence agencies until the Obama administration, was never even considered for Third Party status by NSA. The premeditated Israeli attack on the NSA intelligence collection ship, *USS Liberty* in 1967, Mossad's penetration of NSA operations via a spy ring at RCA Corporation in 1995-6, and the damage down by Israeli spy Jonathan Pollard, discovered in 1995, ensured that Israel would never have official access to NSA's intelligence. NSA carefully covered its intercept operations mounted against Israel by having NSA Hebrew linguists described as being proficient in "Special Arabic."

Keeping Israel removed from NSA operations all changed under the Obama administration when a Memorandum of Understanding was drafted between NSA and the Israel SIGINT National Unit (also known as Unit 8200 or *Yehida Shmoneh-Matayim*) to share highly-classified SIGINT data. France's relationship with NSA graduated from Third Party to a category that can be described as Third Party plus. NSA SIGINT and Communications Intelligence or COMINT material was marked with the special caveat REL TO USA, FRA if it was authorized to be released to France. Likewise, Israel appeared to have received a Third Party plus status since NSA material authorized for release to Israel received a handling category of REL to USA, ISR.

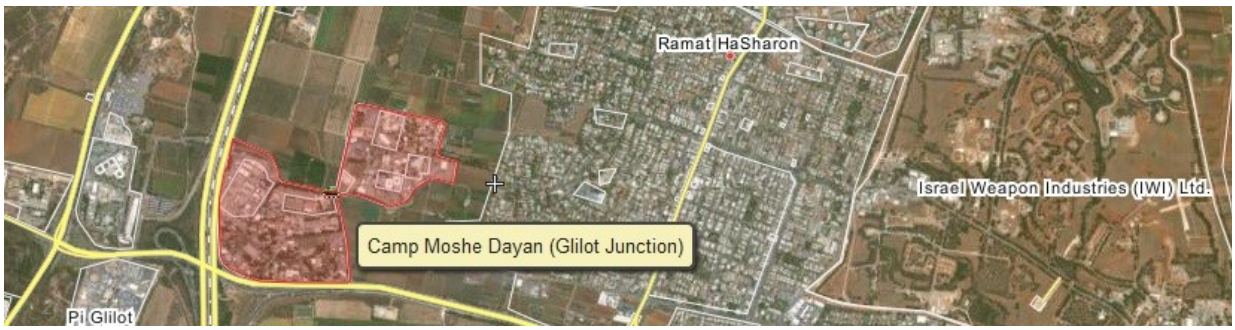
While NSA's control over its "FIVE EYES" English speaking partners was relatively without major incident, aside from a spat with New Zealand in the 1980s over its policy of refusing to allow U.S. nuclear-powered warships into its waters, the same was not the case with Israel and France.

The TOP SECRET//COMINT//REL to USA, ISR (but not releasable tol FIVE EYES) MOU with ISNU not only permitted NSA SIGINT, including raw intercept traffic, to be shared with Israel but also stipulated that SIGINT collected by the FIVE EYES alliance could also be shared with the Israelis. However, the other four members of FIVE EYES were not included in the releasing authority granted by the NSA-ISNU memorandum. ISNU was merely "requested" in the MOU to protect the SIGINT handling laws and regulations of the FIVE EYES countries. [Excerpt of the MOU below].

The nature of ISNU's special relationship with NSA was highlighted by the description of the duties of SUSLAIS (Senior U.S. Liaison Adviser Israel) in the MOU. The SUSLAIS, similar to the SUSLO (Senior U.S. Liaison Officer), officially attached to the U.S. embassy in London but assigned to work closely with the UK Government Communications Headquarters (GCHQ) in Cheltenham, England, was to handle any discovery by the Israelis of raw data on U.S. persons foud in raw intercept traffic provided to ISNU. The MOU does not make it clear what kind of access, if any, the SUSLAIS has to ISNU facilities located at Camp Moshe Dayan at Glilot Junction, north of Tel Aviv and near Herzliya.

ISNU was also charged with requesting permission from NSA, presumably through the SUSLAIS, before releasing NSA SIGINT data to any other party, which would include the Mossad, Shin Bet, or other Israeli government agencies. The MOU also refers to a special NSA-ISNU shared communications network codenamed CHIPPEWA.

יחידה 8200



Location of NSA's problematic Israeii partner, Unit 8200.

Israel had been caught over the past decade trafficking in stolen or forged passports from Australia, Britain, New Zealand, and Canada. However, the NSA and the Obama administration concluded that Israel could be trusted with highly-classified SIGINT and COMINT from the intelligence agencies of countries subjected to Israeli intelligence operations.

(TS//SI//REL) This agreement will apply to any SIGINT raw traffic, technology, or enabling that NSA may provide to ISNU. This agreement applies only to materials provided by NSA and shall not be construed to apply to materials collected independently by ISNU.

(TS//SI//REL) ISNU also recognizes that NSA has agreements with Australia, Canada, New Zealand, and the United Kingdom that require it to protect information associated with U.K. persons, Australian persons, Canadian persons and New Zealand persons using procedures and safeguards similar to those applied for U.S. persons. For this reason, in all uses of raw material provided by NSA, ISNU agrees to apply the procedures outlined in this agreement to persons of these countries.

It was not long before Israel began taking advantage of its new relationship with NSA and its Second and Third Party partners. In April 2013, the French discovered that "cyber-attacks" were taking place against the French Presidential communications network.The French Directorate for External Security (DGSE) requested and received a meeting with senio0r NSA officials at NSA Headquarters in Fort Meade, Maryland. The meeting, held on April 12, 2013, was attended by Bernard Barbier, the Technical Director of DGSE, and Patrick Pailloux, the Director of the National Information Systems Security (ANSSI) unit of France. The information on the attack is contained in an overall TOP SECRET//SI//NOFORN, meaning No Foreign Nationals memo issued by NSA for the visit. DGSE and ANSSI first informed NSA director Lt. Gen. Keith Alexander about the cyber-attacks in January 2013 during a visit by Alexander to Paris. Alexander was prepared to send two NSA Threat Operations Center analysts to France to investigate. DGSE and ANSSI told Alexander about the cyber-attacks without going through the SUSLAF (Senior U.S. Liaison Activity France) or NSA's FAD (Foreign Affairs Directorate). Rather than receiving NSA analysts in France, DGSE and ANSSI opted, instead, to visit Fort Meade.

The NSA memo on the French visit only authorized for release to France (REL TO FRA) information on the visit of the two French officials to NSA. The unclassified reason for the visit was "Computer Network Defense."

The NSA organization charged with conducting cyber-attacks, Tailored Access Operations or TAO denied that the operations against the French Presidential network was their work. TAO, which includes personnel with the joint NSA-CIA Special Collection Service (SCS), inquired among "First Parties," that is the CIA, and "Second Parties," the UK's GCHQ and the Communications Security Establishment Canada (CSEC) whether they were responsible for hacking the French network as they "were the most likely suspects," but they denied any involvement. The memo then states something vitally critical" "TAO did not ask either the Mossad or ISNU whether they were involved as France is not an approved target for joint discussion." In other words, NSA's compartmented security controls did not permit Israel to know anything about any

NSA, GCHQ, or CSEC cyber-espionage against France. However, it is clear that NSA officials believed that Israel might have been the culprit behind the attacks on the French presidential network.

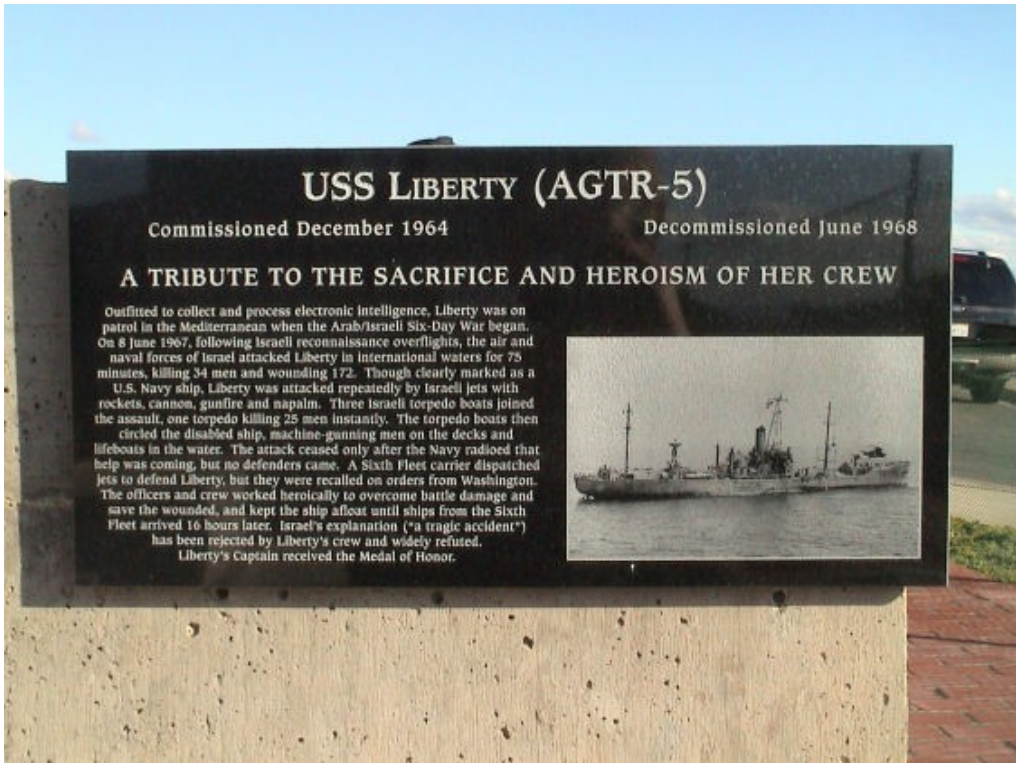
- (TS//SI//NF) TAO confirmed that this was not a TAO operation. TAO asked most of NSA's close 1st/2nd Party Partners whether they were involved (CIA, GCHQ, and CSEC were the mostly likely suspects); everyone has denied involvement. TAO intentionally

did not ask either Mossad or ISNU whether they were involved as France is not an approved target for joint discussion.

There has been an obvious breakdown in internal security at NSA arising from inviting Israel to the SIGINT table. This scenario happened before. In the 1980s, the Reagan administration authorized NSA to help Israel build a SIGINT system based on the use of tethered aerostats (dirigibles) on Israel's borders. The project, codenamed DINDI, was contracted to RCA engineers in Mount Laurel, New Jersey. However, it was soon discovered that some Jewish RCA engineers were violating NSA security controls by sharing NOFORN U.S. national security SIGINT information with Israeli engineers. A damage assessment by NSA concluded that sensitive NSA systems, including PIEREX, MAROON SHIELD, and MAROON ARCHER had been totally compromised to the Israelis. The FBI was prepared to bring criminal charges but the sensitivity surrounding the cooperation of a number of Jewish-American engineers prevented criminal charges from being filed. This event occurred at the same time Israeli spy Jonathan Pollard was charged with handing Israeli intelligence agents a garage-full of classified documents from the Naval Intelligence Support Center in Suitland, Maryland.

The information that NSA possessed on Israel's hostile intelligence threat necessitated a change of thinking for Israeli intelligence. Rather than deal with crises over Israeli intelligence penetration of NSA, it chose to place its supporters and sympathizers within the NSA hierarchy. This strategy hit pay dirt with the NSA-ISNU MOU. But even beforehand, one NSA sympathizer, NSA General Counsel Robert L. Deitz, was responsible for countering charges that Israel had launched an unprovoked attack on the *Liberty* in 1967. One of Deitz's major tasks was to ensure that the survivors of the Israeli attack on the *Liberty*, which killed 34 U.S. Navy and NSA personnel, were never able to obtain NSA SIGINT evidence, including translations of Hebrew intercepts, proving that Israel's attack was willful and designed to actually sink the ship with all hands lost at sea.

After Congressman Eric Massa (D-MY) visited the new *USS Liberty* Memorial in Rochester, New York, he was targeted in a vicious and defamatory campaign launched by then-White House chief of staff Rahm Emanuel, the son of an Israeli Irgun gang terrorist, and Barney Frank (D-MA), a major supporter of Israel. Massa was accused, without proof, of engaging in improper behavior with male staffers. One of Massa's chief accusers, a member of his staff, had previously been an aide to Frank, a married gay man with a scandalized past involving during his earlier time in the House of Representatives. Amid the unsubstantiated charges against him and media frenzy, Massa resigned from office.



USS Liberty Memorial in La Jolla, California. Israel's agents of influence inside NSA have ensured the ship remains a

forgotten "footnote" in NSA's history

Israel also relies on a network of sympathizers and propagandists to carry its water on the Internet. This is accomplished mainly through the Megaphone desktop tool employed by the Israeli group Give Israel Your United Support (GIYUS).

Ever since Edward Snowden's disclosures about NSA, there has been a Twitter frenzy involving U.S. government officials defending not only NSA but Israel. One particular hot button issue is the NSA-ISNU relationship. One particular critic of those who defend Snowden and oppose NSA's surveillance powers is U.S. Naval War College Professor John Schindler who describes himself as a former NSA intelligence and counterintelligence officer. Schindler presides over a group of Twitter followers who assist him in attacking NSA critics. The Twitter exchange below is but one example.

Dan Murphy @bungdan 6h
Pop quiz: In what foreign city was the bulk of the operational planning for the 9/11/2001 attacks on New York and DC done?
View details ·

John Schindler **John Schindler** **Follow**
@20committee

.@bungdan You're gonna say Hamburg, you imperialist lackey, when we all really know it's Tel Aviv. And by "we all" I mean Wayne Madsen.
7:43 a.m. Sun, Oct 27

Considering Israel's nefarious past with NSA, those NSA insiders who wear loyalty to Israel on their sleeves should at least be availed the courtesy of a rudimentary counterintelligence special background check.

Back to top Previous | Next